INTERNATIONAL SEARCH REPORT

International application No.

PCT/US04/21847

	International Patent Classification (IPC) or to both sa DS SEARCHED	nonas Glassiicanini ano 12 C	
	icumentation searched (classification system followed b 713/171,193,194, 380/203.210,259,273,37,281; 379/12		AND THE PERSON OF THE PERSON O
locumentati	on searched other than minimum documentation to the	extent that such documents are included to	the fields searched
Bectronic d	are base consulted during the international search (name	e of data base and, where practicable, sear	ch terms used)
000	TIMENTS CONSIDERED TO BE BELEVANT		
ategory *	Citation of document, with indication, where a	enropriate of the relevant pastwork.	Relevant to claim No.
X	X US 2001/0029581 (KNADFT) 11 October 2001 (#514, Fig. 5B, #522	(11.11.2001), \$48, \$75-86, Fig. 5A.	1-39
X.P 7.P	US 6,690,795 B1 (RICHARDS) 10 February 2004,	columns 5-10.	1-39
Х Y	US Re. 33,189 (LEE et al) 27 March 1990 (27.03.1 36.	990), colums 2, line 37 - column 4, line	t-39
Y	MENEZES et al. Handbook of Applied Cryptograp Mathematics and its Applications, BOCA Raton, FL 557-581.		1-39
1400	or documents are fisted in the continuation of Box C.	See potent family annex.	omedowal falcos dans or priority
A" documen	or documents are fisted in the continuation of Box C. Speem caugement clear december, to defining the general tase of the an which is my combined to be user terminal.	"I" isser stocument published after the inte- date and not in conflict with the applic principle or theory noterlying the inte	amon but nated on understand it minim
A" document of parties	Special transpores of client documents at Offining the general state of file an which is not considered to be while televation policies on povent published on an after the transported filing date	"Y" lister document published after the lister date and not in conflict with the replic	acion but ested so understand is seion cisimed instruive traces be
A" document of parties E" destiner a	Special calegores of clied documents at defining the general state of the ani which is more consisted to be user reference or preference and the consisted to be user reference specialism or private preference and after the transmissional filling dise or which may throw thereby on private planting or which it cause to the problemation district of number criticine moving resident private planting the problemation district of number criticine moving resident private the problemation district of number criticine moving resident private the problemation district of number criticine moving resident private the problemation district of number criticine moving resident private the problemation districts.	"y" Issee document published after the time date and not in conflict with the applic principles on theory indicated on the application and the application of the application and application	cation because as understand a scious claimed investment cannot be and to suvestme as investive asse- claimed investment cannot be a when the choositest in
A" documes of partie E" destiner a L" documes equilitat specified O" decomes	Special craegeries of cloud decembers; six definings the general raws of the as which is may considered to be user technical six technical control of the production of the state of the consideration of the policy of the production of the state of the consideration of the production of the production duties of models exclusive are other special examine as all of excitations as as to make decision and the state of models exclusive are other special examine as a fine of the production of the state of models exclusive are other special examine as a fine of the state of models exclusive, see, exhibitions on other examine.	197 ister document published states the bind date and not be certified visit the comparison of the com	account that cated an understand is probed involves to account to most on unwater are inventive use claimed inventions control to y about the document is a populariams, such conditionation or are
A" document of passic E" destiner a L" document establish specified O" document probitity	Special is response of clad discenses; studingly also general tase of the six which is not considered to be use inclusion. Specialistic or syntax perialistic on an afair the numerous affiling disce and continuity of the continuity or six and expedit invente tase of smother continuity or six and expedit invente tase of smother continuity or six and expedit invente tase of smother continuity or six and the continuity or six and discinuity, saw, exhibitions or other sensus as publicular given to the international filling date but have than the direct continuity.	197 into faccarea guidaded atter the use date and not in certifial with the epid- springed on theory solerlying the Circ. *** **destinated of platification extends of the conditional of platification extends or conditional when the documents is basical attention when the conditional neutral soler in the conditional neutral soler in the conditional neutral soler in the conditional in aircraft as in the resemble soler conditional wind neutral resemble conditional in aircraft as in the conditional wind neutral resemble soler in the conditional wind neutral resemble soler in the conditional soler in the condition of t	assous that cause so understand is maken. Claimed law-thinks classes for and to surviving an investigation are claimed law-poison control to y where the document is a properties, such conditionation or are
A" document of parties E" eather a document specified O" document profits; Date of the s	Special i criegione el clade discenses; se definitiva de general taxe of the six volto di ma consistent de be ser formano de general taxe of the six volto di ma consistent de be glicitation or porter perificiano ser si fair de communità d'alleg des serviciones della del privincy discensor que vinche i que so se policitatione della del similario continuo er notere questi creaso se se reforma più se mal discionare, servicione della servicione se reforma più se mal discionare, servicione della servicione se publicatione della granda della servicione se publicatione processor della servicione se publicatione processor della servicione se publicatione processor della servicione servicione della servicione servic	137 ison forceron guidalized atter the use date and not be centillar with the spirit control of the control of	assous that cause so understand is maken. Claimed law-thinks classes for and to surviving an investigation are claimed law-poison control to y where the document is a properties, such conditionation or are
A" document of parties of parties of parties of parties of parties of parties of the state of th	Special is useganis of clinal disciences; as commission of clinal disciences; as in clinarias of the six which is not consistent to the positions of my meta pelitidate are all and the commissional filling disc productions of the commission of the commission of the discience of the commission of the commission of the discience of the commission of the commission of the pelitidate price to the intervolution filling date but have the discience of the commission of the commission of the commission of the commission of the commission of the commission of the commission of the discience of the commission of the commission of the commission of the commission of the commission of the commission of the commission of the commission of the commission of the commission of	137 ister forceron published after the use date and not in centiliar with the application of the transport of the publication of publication of publication of the considered aboved to cannot be considered when the documents of publication retrievancy and considered and interview as transferred to interview as the considered and interview as t	assous that cause so understand is maken. Claimed law-thinks classes for and to surviving an investigation are claimed law-poison control to y where the document is a properties, such conditionation or are
A" document of particle to the control of particle to the control of the control	Sports' interests of third documents. Gotting the general state of the an which is may consistent to be the selection of the	137 issue decrease galatitied attent the same date and on it certifies with despite galatine and the incertifies with the spite galatine and the incertifies with the spite galatine and the incertifier and the considered made of a second to consider a considered made of particular sections of a second to consider a considered made of a second to considered made of the second to considered ma	asions the citation of understand is existen. Cisimed interestion isonous lies not on an other as invertices asse- cial and assessment can be citational interesting the control in a deposition of the control in a deposition of the control in a dep
A" document of partie E" detrier a document specialists specialists of the common priority. A " document specialists of the common priority. A November 1 M. M. Co. P. 9.	Special statement of third documents on the constituted to be the constituted to the co	The state of the s	asions the citation of understand is existen. Cisimed interestion isonous lies not on an other as invertices asse- cial and assessment can be citational interesting the control in a deposition of the control in a deposition of the control in a dep
A" documes of partie E" statier a E" documes souldain specified O" documes printity Otto Of the a 8 Novembe Same and a L' document Same and a L' document Same and a L' document L' document Same and a L' document A L' docu	Special integration of Claid deceasing. (offining in general state of the air which is may consistent to be described in the control of the	137 issue decrease galatitied attent the same date and on it certifies with despite galatine and the incertifies with the spite galatine and the incertifies with the spite galatine and the incertifier and the considered made of a second to consider a considered made of particular sections of a second to consider a considered made of a second to considered made of the second to considered ma	asions the citation of understand is existen. Cisimed interestion isonous lies not on an other as invertices asse- cial and assessment can be citational interesting the control in a deposition of the control in a deposition of the control in a dep

PATENT COOPERATION TREATY

REC'D 2 9 DEC 2004

tom the	TONAL SEARCE	HING AUTH	ORITY		WIPO	
KIERNATIONAL SEARCHING AUTHORITY To: MILAN PATEL 5775 MOREHOUSE DRIVE SAN DIEGO, CA 92121-1714				PCT WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY		
					(PCT Rule 43bis.1)	
				Date of mailing (day/month/yeur)	23 DEC 2004	
Applicant	's or agent's file r	eference		FOR FURTHER.	ACTION See paragraph 2 below	
030441WO			120		Priority date (day/month/year)	
	ual application No		International filing date			
PCT/USO Internation	4/21847 nal Patent Classifi	cation (IPC)	08 July 2004 (08.07.200 or both national classificat		68 July 2003 (08.07.2003)	
IPC(7): H		11/30,12/14,5			1/06 and US Cl.: 713/171,193,194;	
HAWKES	ET AL.					
I. This	This opinion contains indications relating to the following items: Box No. I Basis of the opinion					
	Box No. II	Priority				
	Box No. III	Non-establi	shment of opinion with re	gard to novelty, inve	entive step and industrial applicability	
	Box No. IV	Lack of uni	ity of invention		***************************************	
\boxtimes	Box No. V					
	Box No. VI	Certain doc	ruments cited			
	Box No. VII	Certain des	ects in the international ap	plication		
\boxtimes	Box No. VIII	Certain obs	ervations on the internation	nal application		
2 171112	THER ACTIO	N				
If a d Inters Auth	lemand for interm national Prelimina prity other than th	ational prelim iry Examinin	ig Authority ("IPEA") e:	cept that this does IPEA has notified th	be considered to be a written opinion of the not apply where the applicant chooses an e International Bureau under Rule 66 1bis (b) iered.	
IPEA maili	a written realy	together, wh ISA/220 or b	ere appropriate, with an efore the expiration of 22	endments, before the	PEA, the applicant is invited to submit to the ac expiration of 3 months from the date of ority date, whichever expires later.	
rori	andr options, se	o rouse FCI/	mesende.			
3. For f	urther details, see	notes to For	m PCT/ISA/220.			
	mailing address of		IS	Authorized office		
Mail Stop FCT, Ann. ISA/US Cummissioner for Patents P.O. Box 1450				Greg Morse	eggy Hanod	
Adexaofria, Virginia 22313-1450 Facsimile No. (703) 305-3230				Telephone No. (571) 272-3838		

Form PCT/ISA/237 (cover sheet) (January 2004)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCI/US04/21847

Box No	3. I	Basis of this opinion
	file	rd to the language, this opinion has been established on the basis of the international application in the language in which t, unless otherwise indicated under this item. The proposed is the proposed on the basis of a translation from the original language into the following language
	whi	ch is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).
		rd to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the vention, this opinion has been established on the basis of:
a.	typ	e of material
		a sequence listing
		table(s) related to the sequence listing
ъ.	for	mat of material
		in written format
		in computer readable form
c.	tim	e of filing/furnishing
		contained in international application as filed.
		filed together with the international application in computer readable form.
		furnished subsequently to this Authority for the purposes of search.
3. 🗌	file	addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been d or furnished, the required statements that the information in the subsequent or additional copies is identical to that in application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additi	ional	comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US04/21847

Box No. V Reasoned statement under Rule 43 bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement				
Statement				
Novelty (N)	Claims	1-39		
	Claims	NONE	NO	
Inventive step (IS) Industrial applicability (IA)	Claims NONE	NONE	YE	
	Claims		N(
	Claims NONE	YE		
that approximity (a t)		NONE	NC	
Citations and explanations:				
ease See Continuation Sheet				

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.

PCT/US04/21847

Box No. VIII Certain observations on the inte	ernational application
---	------------------------

The following observations on the clarity of the claims, description, and drawings or on the questions whether the claims are fully supported by the description, are made:

Regarding claims 5, 13, 19, 25, 31 & 37, "the secret key" does not appear in the claim or any of it's depending claims. The references to "the secret key" are understood to mean "the access key" in these claims.

Form PCT/ISA/237 (Box No. VIII) (January 2004)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US04/21847

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

Claims 1-39 lack inventive step over U.S. Patent Re. 33,189 to Lee et al. (Lee) in view of Handbook of Applied Cryptography by Menezes et al. (Menezes).

Regarding claims 1, 16 & 28, Lee discloses distributing a key/kset ID (col. 3, lines 28-42), receiving a secret key encrypted by the key/kset ID (col. 4, lines 1-22), encerying the secret key/key (col. 4, lines 1-22), neelving the secret key/key (col. 4, lines 1-22), receiving the secret key/key (col. 4, lines 1-22). The property of the secret key/key (col. 4, lines 1-22), receiving the secret key/key (col. 4, lines 1-22). The secret key/key (col. 4, lines 1-22) and dearypting the access key/random number by the secret key/key (col. 4, lines 1-22). The secret key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt of the characteristic form of the secret key is distributed, key-encrypting keys are used to transport keys and data keys are used to encrypt often keys, which are the decrypted by the corresponding private key (n. 552, #2 & Fig. 13.4(b)). Therefore, it would have been obvirus to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as taught by Menzezes (p. 551, #1.3).

Regarding claims 2, 8, 11, 15, 17, 21, 23, 27, 29, 33, 35 & 39, Lee discloses the secret key being a temporary key/key of the month (col. 3, lines 28-42).

Regarding claims 3 & 9, Lee discloses deriving a short key/PN sequence based on the access key/random number, receiving energined broadcast content/video and decrypting the encrypted broadcast content using the short key/PN sequence (col. 3, line 28 - col. 4, line 27).

Regarding chims 4, 18 & 30, Lee discloses distributing a key/user ID (col. 3, lines 28-42), receiving the access key/key encrypted by the key/user ID and derrypting the access key/key by the private key/user [00.04, 4 lines 1-22]. A lee lacks a pulce lexy. However, Memross teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting keys are used to transport key and data keys are used to encrypt the data a user will use [0, 552-553, 813,13]. Specifically, Menczes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552,82,82,82) at [24,69). Thisrefore, it would have been obvious to me having ordinary skill in the art at the time the twentions made to use a public key to encrypt the screet key. One of ordinary skill in the art at whe time the twention conditional to achieve simplified key management, as taught by Memcree, [0, 551, 47.3].

Regarding claims 5, 13, 19, 25, 31 & 37, as best understood, Lee discloses the access key being a temporary key (key of the month) (col. 3, lines 28-42).

Regarding claim 6, Lee discloses deriving a short keyfrandom number based on the access key/key, receiving entrypted broadcast content/video and decrypting the entrypted broadcast content/video using the short keyfrandom number (col. 3, line 28 - col. 4, line 22).

Regarding claims 7, 20 & 23, Lee disalows receiving a key/user ID corresponding to a private key/user ID (col. 3, lines 28-42), encryping the secret key/key with the key/user ID (col. 3, lines 42-64), sending the encrypted secret key/key (col. 3, lines 12-6, receiving the access key/random member encrypted by the secret key/key (col. 4, lines 1-22) and decrypting the access key/random number by the secret key/key (col. 3, line 28-col. 4, line 22). Lee lacks a public key. However, Menteze teaches that key layering is a key-exchange technique, whereby a matter key is distributed, key-encrypting keys are used to transport keys and data keys a

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No. PCT/US04/21847

Supplemental Box

in case the space in any of the preceding boxes is not sufficient.

used to encrypt the data a user will use (pp. 552-553, §13.3.1). Specifically, Menezas teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 552, £76 Fig. 13-40b). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve simplified key management, as faught by Menezee (p. 551, £7-3).

Regarding claims 10, 22 & 34, Lee disoloses receiving a kerylater ID (col. 3, lines 26-47), excrypting a secret kerylkery using the kerylater ID (col. 3, lines 42-64), sending the encrypted secret keylker (col. 4, lines 1-5), encerypting the access keylrating number using in the secret keylyker (col. 4, lines 1-26) and sending the encrypted access keylrating mumber (col. 4, lines 1-22). Lee lacks a public key. However, Menezes teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encrypting key are used to returned key as concept the data at user will use (pp. 532-553, §13.3.1). Specifically, Menezes teaches that public keys can be used to encrypt other keys, which are then decrypted by the corresponding private key (p. 52, & & & & Fig. 13-40). Therefore, is would have been onlyout to use having ordinary skill in the car at the time than the invention was made to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a notification to achieve simplified key management, as taught by Meazers (p. 531, #1-3).

Regarding claims 12, 24 & 26, Lee dischors recolving a key/neer ID (onl. 4, lines 1-22), encrypting the access key/neer using in key/neer ID (onl. 5, lines 2-46). Lee tables a public level using in key/neer ID (onl. 5, lines 2-46). Lee tables a public level using the key/neer ID (onl. 5, lines 2-46). Lee tables a public level can be used to many the principle in a key-exchange rechnique, whereby a manter key is distributed, key-excepting keys are used to meany they and table keys can be used to encrypt they are used to encrypt the data a user will us (op. 95-255, \$1 \$1.3.1.1). Septicifically, Memories teaches that public keys can be used to encrypt odder keys, which are then decrypted by the corresponding private key (or. 552, #2 & F1g. 13.4(b)). Therefore, it would have been onlying to one having ordinary skill in the art at the time the invention was made to use public keys to encrypt the secret key. One of ordinary skill the art would have been motivated to perform such a modification to entire vestigation (ever management, as taught by Memories (9, 552, #2).

Regarding claims 14, 26 & 38, Lee discloses distributing a keyluser ID corresponding to a private keyluser ID (col. 3, lines 24-24), receiving a securit keylvse (col. 3, lines 24-26), deepting a securit keylvse (col. 3, lines 24-26), deepting the secret keylvse (col. 3, lines 24-26), deepting the secret keylvse (col. 3, lines 24-26), deepting the secret keylvse (col. 3, lines 24-26), and senting the energy-set security (col. 3, lines 1-22), enterpying the access keyl-random number by the secret keylvsey (col. 3, lines 24-26), and senting the energy-set secases keyl-random number (col. 3, line 28-20, ed., line 22). Len lucks a public key. However, Menezon teaches that key layering is a key-exchange technique, whereby a master key is distributed, key-encypting keys are used to transport keys and that keys are used to encrypt the data a user will use (pp. 55-25-58, 183.3). Specifically, Menezos teaches unbile keys can be used to sucrypt other keys, which are then deerypted by the corresponding private key (p. 552, #2 & Fig. 13.4(b)). Therefore, it would have been divinest to one having ordinary skill in the art would have been divined to use a public key to encrypt the secret key. One of ordinary skill in the art would have been motivated to perform such a modification to achieve semblified key management, as taught by Menezos e.5.5. #1.9-13.

US Re. 33.189 (LEE et al) 27 March 1990 (27.03.1990), column 2, line 37 - column 4, line 36.

MENEZES et al. Handbook of Applied Cryptography, CRC Press Series on Discrete Mathematics and its Applications, BOCA Raton, FL, CRC Press, US, 1997, pp. 551-553, 557-581.